REMARKS

Entry of this Amendment is proper because it does not raise any new issues requiring further search by the Examiner, narrows the issues on appeal, and is believed to place the present application in condition for immediate allowance.

Claims 1-27 are all the claims presently pending in the application.

Applicants specifically state that no amendment to any claim herein, or previously submitted, should be construed as a disclaimer of any interest in or right to an equivalent of any element or feature of the amended claim.

Claims 1-27 stand rejected on prior art grounds.

With respect to the prior art rejections, claims 1, 3-7, 9, 13, 24, 25, and 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek (U.S. Patent No. 5,933,501) in view of Maillard et al. (U.S. Patent No. 6,466,671; hereinafter "Maillard"). Claims 2, 10-12, 14, 23, and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard, and further in view of Perlman et al. (U.S. Patent No. 5,261,002; hereinafter "Perlman"). Claims 8, 15-18, and 20-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard, and further in view of Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Second Edition, pps. 466-474 (hereinafter, "Schneier"). Claim 19 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard, and further in view of Schneier, and further in view of Perlman.

These rejections are respectfully traversed in the following discussion.

I. THE CLAIMED INVENTION

The claimed invention relates to a method and system for producing wise cards.

In an illustrative, non-limiting embodiment of the invention, as defined by independent claim 1, a method of preventing counterfeiting of a smart card includes providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined small number of readings, wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof.

In conventional methods and systems, counterfeiting/duplication is not rendered difficult since confidential information is carried on the card and an unscrupulous person may find the information simply by looking at or reading the energy construction inside of the card. That is, with a plurality of readings of the card, the information held within the card can be easily detected (e.g., see specification at page 3, line 19, to page 4, line 2).

The claimed invention, on the other hand, complements the conventional smart-card-type of security, which is often all carried on the card itself, by providing extra protection depending on cryptography, with the cryptographic structure (e.g., a key) not being carried by the card and which cannot be accessed completely by a predetermined small number of readings. Moreover, the cryptographic structure can only be built by whoever emits the card or the agent thereof (e.g., see specification at page 4, lines 9-13).

The claimed invention, in addition to preventing the creation of false cards different from the legitimate ones, also prevents the fabrication of clones of a given legitimate smart card. That is, the present invention also provides a mechanism of protection designed to prevent and/or discourage both copying and creation of new cards (e.g., see specification at page 4, lines 14-17).

II. THE PRIOR ART REJECTIONS

A. Claims 1, 3-7, 9, 13, 24, 25, and 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard.

In the Response to Arguments, the Examiner states that the Examiner disagrees with Applicants. Particularly, the Examiner states that:

> *As per the interview on September 1, 2004, examiner portrayed his opinion as to why it would be obvious to combine the Leppek and Maillard reference. The idea was that Leppek taught the concept of not exhausting the entire list of cryptographic keys with one, or even a few, readings. This would prevent an intruder from learning the cryptographic technique used. The idea of combining it with a smart card, from Maillard, is obvious in that technology tends to put once large processing components into smaller and smaller devices.*

(see Office Action at pages 19-20, bridging paragraph; emphasis added).

Applicants respectfully submit, however, that it would not have been obvious to combine the cited references in the manner alleged in order to arrive at the claimed invention. Moreover, Applicants submit that there are elements of the claimed invention which are not disclosed or suggested by Leppek or Maillard, alone or in combination. Therefore, Applicants respectfully traverse this rejection.

As the Examiner surely knows, the references as a whole must be considered for what they fairly teach to the ordinarily skilled artisan. Moreover, merely identifying individual elements of the claims in separate references is not sufficient to establish the obviousness of the claims. The Office Action must establish a reasonable motivation or suggestion, in the references themselves or in the art in general, for combining the references to arrive at the claimed invention. The mere fact that references could (or can) be combined or modified is not sufficient to establish *prima facie* obviousness (see M.P.E.P. § 2143.01). There must be a

reasonable motivation, in the references themselves or in the art in general, to do that which the patent applicant has done.

Moreover, to render the claims obvious, there must also be a reasonable expectation of success and the prior art references, when combined, must teach or suggest all of the claim limitations (e.g., see M.P.E.P. § 2142). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, ***not*** in Applicant's disclosure (see M.P.E.P. § 2143, *citing* In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

Applicants respectfully submit that there are clear distinctions between Leppek and Maillard (or for that matter, any combination thereof), and the features of the claimed invention. Indeed, other than involving some form of cryptography, the individual references (or alleged combination thereof) have nothing to do with the claimed invention or the problems being solved by the claimed invention.

In fact, Leppek and Maillard do not even contemplate or mention the problems addressed and solved by the claimed invention, or for that matter, the advantages derived from the novel and unobvious method according to the claimed invention.

For example, Leppek specifically states that it is directed primarily to "*a prescribed set of communication encryption and decryption software employed by digital data terminals (sic) and communication equipment, that effectively enables end users of a data communications link to conduct secure data communications therebetween without the practical possibility of successful recovery in an intercepted encrypted data*" (see Leppek at column 3, lines 24-34; emphasis added).

In other words, Leppek merely uses cryptographic schemes to protect secret messages. Leppek does not, however, disclose, suggest, or even mention preventing counterfeiting or cloning a physical instrument (e.g., a smart card) by authorizing the physical instrument.

On the other hand, Maillard merely teaches a smart card for use with a receiver of encrypted broadcast signals including a microprocessor for enabling controlling decryption of the signals (e.g., see Maillard at Abstract; emphasis added).

As with Leppek, Maillard merely uses cryptographic schemes to protect secret messages. In fact, Maillard specifically states that:

> *[t]he smartcards contain the secrets of one or more commercial operators. The "mother" smartcard encrypts different kinds of messages and the "daughter" smartcards decrypt the messages, if they have the rights to do so.*

(see Maillard at column 6, lines 55-58; emphasis added).

At best, the combination of Leppek and Maillard would be a smart card which uses the cryptographic schemes of Leppek to protect secret information or messages on the smart card of Maillard. However, this resulting combination merely is comparable to conventional cryptographic schemes used with smart cards to protect the information on the smart card.

In stark contrast, the present invention provides a novel and unobvious method of preventing counterfeiting (i.e., false smart cards or illegitimate cards) and/or preventing cloning (i.e., copies of legitimate smart cards or counterfeit smart cards) of a smart card by authorizing (e.g., verifying the legitimacy of) the smart card. That is, the claimed invention provides a simple and effective solution to problems with conventional smart cards which use cryptographic schemes merely to protect secret information or messages on the smart card itself, but do not

authorize or authenticate a smart card (i.e., do not prevent counterfeiting and cloning of a smart card).

Leppek and Maillard, either alone or in combination, clearly to do not disclose or suggest the features of the claimed invention.

For example, the claimed invention, as defined for example by independent claim 1, provides a "method of preventing counterfeiting of a smart card, comprising: providing a smart card with a cryptographic structure for ***authorizing*** the smart card which cannot be accessed completely by a predetermined small number of readings, wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof" (emphasis added).

Thus, the claimed invention complements the conventional smart-card-type of security, which is often all carried on the card itself, by providing extra protection depending on cryptography, with the cryptographic structure (e.g., a key) not being carried by the card and which cannot be accessed completely by a predetermined small number of readings. Moreover, the cryptographic structure can only be built by whoever emits the card or the agent thereof (e.g., see specification at page 4, lines 9-13).

In this way, the claimed invention, in addition to preventing the creation of false cards different from the legitimate cards (i.e., illegitimate cards), also prevents the fabrication of clones of a given legitimate smart card. That is, the present invention also provides a mechanism of protection designed to prevent and/or discourage both copying and creation of new cards (e.g., see specification at page 4, lines 14-17).

Accordingly, Applicants respectfully submit that it would not have been obvious to combine the cited references in the manner alleged in order to arrive at the claimed invention.

First, as mentioned above, the Examiner states that "*[t]he idea was that Leppek taught the concept of not exhausting the entire list of cryptographic keys with one, or even a few, readings. This would prevent an intruder from learning the cryptographic technique used. The idea of combining it with a smart card, from Maillard, is obvious in that technology tends to put once large processing components into smaller and smaller devices*" (see Office Action at pages 19-20, bridging paragraph; emphasis added).

Applicants respectfully submit, however, that it would not have been obvious to modify Leppek based on Maillard to arrive at the novel and unobvious combination of elements recited in the claimed invention.

As mentioned above, the mere fact that references could (or can) be combined or modified is not sufficient to establish *prima facie* obviousness (see M.P.E.P. § 2143.01). There must be a reasonable motivation, in the references themselves or in the art in general, to do that which the patent applicant has done.

Applicants respectfully submit that it would not have been obvious to modify Leppek based on Maillard to arrive at the novel and unobvious combination of elements recited in the claimed invention simply "*to put large processing components into smaller and smaller devices*", as alleged.

Indeed, that the Examiner has not established, either in the grounds of rejection or in the Response to Arguments, a reasonable basis for such combination of Leppek and Maillard.

Thus, Applicants respectfully submit that the final Office Action fails to reasonably establish the obviousness of the claimed invention as a matter of law.

As another example, in the ground of rejection, the Examiner alleges that it would have been obvious "*to implement the teachings of Leppek onto a smart card, as taught by Maillard et*

al., because smart cards are small, easy to use mediums (sic) for encryption" and because "*a method which prevents a footprint or playback attack (sic) from being performed by an intruder would help spread the acceptance of smart cards used in technology*" (see Office Action at page 4, lines 8-15; emphasis added).

Applicants respectfully submit, however, that it would not have been obvious to modify Leppek based on Maillard to arrive at the novel and unobvious combination of elements recited in the claimed invention, and further, that the Examiner has not established a reasonable basis for such combination of Leppek and Maillard, for several reasons.

Applicants respectfully submit that the Examiner has not explained, nor do the references provide support for, *how* the features relied upon in Leppek, which is *not* a smart card, could (or would) be implemented in a smart card, such as the smart card of Maillard, or for that matter, *how* such a combination would arrive at the claimed invention.

That is, the Office Action fails to establish *how* "*communication encryption and decryption software employed by digital data terminals (sic) and communication equipment, that effectively enables end users of a data communications link to conduct secure data communications*" (see Leppek at column 3, lines 24-34; emphasis added) could (or would) be combined with a smart card for use with a receiver of encrypted broadcast signals including a microprocessor for enabling controlling decryption of the signals (e.g., see Maillard at Abstract; emphasis added) to arrive at the claimed method of preventing counterfeiting or cloning a physical instrument (e.g., a smart card) by authorizing the physical instrument.

Applicants respectfully submit that it is not enough merely to identify (or pick and choose) individual elements from the references and combine them to try to arrive at the claimed invention, with the benefit of Applicants' invention as a guide to such a combination, in order to

establish the obviousness of the claimed invention. The Office Action must establish a reasonable motivation or suggestion, in the references themselves or in the art in general, for combining the references to arrive at the claimed invention.

The present Office Action has not established a reasonable motivation for such a combination and/or modification. That is, merely alleging that it would have been obvious to implement the teachings of Leppek onto a smart card "*because smart cards are small, easy to use mediums for encryption*" and because "*a method which prevents a footprint or playback attack (sic) from being performed by an intruder would help spread the acceptance of smart cards used in technology*", or simply "*to put large processing components into smaller and smaller devices*", is not sufficient to establish a reasonable motivation for combining the references to arrive at the claimed invention, as a matter of law.

Instead, the Office Action must establish a reasonable motivation or suggestion, in the references themselves or in the art in general, for combining the references to arrive at the claimed invention. Absent such a reasonable motivation, it would appear that the Examiner is using improper hindsight based analysis to arrive at the claimed invention.

Thus, for at least the foregoing reasons, Applicants respectfully submit that it would not have been obvious to combine Leppek and Maillard to arrive at the claimed invention, absent impermissible hindsight based analysis. Accordingly, Applicants submit that the prior art rejections fail to establish the obviousness of the claims as a matter of law.

Applicants also submit that there are elements of the claimed invention which clearly are *not* disclosed or suggested by Leppek or Maillard, alone or in combination. Thus, Applicants further submit that, as a matter of fact, the alleged combination of references, even if combined in the manner alleged by the Examiner, would not arrive a the claimed invention.

For example, in the ground of rejection, the Examiner alleges that Leppek discloses "*a method for preventing counterfeiting and cloning of smart cards*" (see Office Action at page 3, numbered paragraph 6).

However, as the Examiner acknowledges, Leppek does not disclose or suggest a smart card (see Office Action at page 4, line 4). Leppek also does not even mention "*preventing counterfeiting and cloning*", as alleged in the Office Action.

The Examiner also alleges that Leppek discloses "*providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined number of readings*", as allegedly disclosed at column 4, lines 8-66, and the Abstract of Leppek.

However, Leppek clearly does not disclose or suggest a smart card, or for that matter, authorizing a smart card (see Office Action at page 4, line 4). That is, contrary to the claimed invention, Leppek does not disclose, suggest, or even mention authorizing a smart card or any other physical instrument.

Instead, as mentioned above, Leppek merely teaches protecting information using encryption schemes, *not* preventing counterfeiting or cloning of a smart card, or in other words, authorizing a smart card. Thus, for at least these reasons, Applicant respectfully submits that the Office Action clearly has mischaracterized Leppek as disclosing a smart card for preventing counterfeiting or cloning.

Also, as mentioned above, the Examiner states that "*[t]he idea was that Leppek taught the concept of not exhausting the entire list of cryptographic keys with one, or even a few, readings*" (see Office Action at pages 19-20, bridging paragraph; emphasis added).

Applicants note that a "list of cryptographic keys" is usual in the conventional art for obliging many key discoveries to get to the secrets.

However, contrary to Leppek, the claimed invention does not include a "list of cryptographic keys". Instead, the claimed invention (as exemplarily defined by dependent claims 4, 8, and 20-22) includes an original list of pairs made by numbers and their encrypted versions (e.g., see specification at page 5, lines 14-15).

On the other hand, the Examiner alleges that Maillard makes up for the deficiencies of Leppek by disclosing a smart card used in communication systems.

However, even assuming *arguendo* that it would have been obvious to combine Leppek and Maillard, Applicants respectfully submit that such a combination still would *not* arrive at the claimed invention.

For example, Leppek teaches using a plurality of secret encryption schemes managed in an "encryption operators database". The idea in Leppek is that most likely the attacker would not know all encryption operators in the database, nor be able to recognize which one is being used to protect some data set in a given communication.

Particularly, Leppek discloses a "virtual" encryption scheme that combines selected ones of a plurality of different encryption operators stored in an encryption operator database into a compound sequence of encryption operators. Data to be transported from a data source site, such as a user workstation, to a destination or data recipient site, is sequentially encrypted by performing a compound sequential data flow through this sequence prior to transmission (e.g., see Leppek at Abstract).

In other words, Leppek is concerned with trying to protect the secret of messages being transmitted (i.e., secret within messages).

Applicants respectfully submit that this sort of combination of encryption scheme is in fact well known (and is the typical sort of ideas everyone thinks about early on when exposed to the issues of cryptography). Such encryption schemes are usually considered as potentially dangerous among cryptographers, who generally prefer more solid, simple algorithms to complex combinations that may prevent effective testing of the strength of the protection, while creating an illusory sentiment of an acceptable safety level.

Thus, as mentioned above, Applicants respectfully submit that (at best) the combination of Leppek and Maillard would be a smart card which uses the cryptographic schemes of Leppek to protect secret information or messages being transmitted using the smart card of Maillard. However, this resulting combination merely is comparable to conventional cryptographic schemes used with smart cards to protect the information on the smart card.

In comparison, in the claimed invention, rather than trying to protect the secret of (i.e., secret within) messages, the claimed invention authenticates or authorizes the smart cards that are built according to the claimed invention.

Thus, the present invention is of a very different nature than Leppek and/or Maillard, and addresses distinctly different problems and solutions. Contrary to Leppek or Maillard, the claimed invention provides protection for a smart card on top of (i.e., in addition to) rather widely known technologies and practices, such as those in Leppek, or for that matter, in Maillard.

For the foregoing reasons, Applicants respectfully submit that it would not have been obvious to combine the cited references in the manner alleged in order to arrive at the claimed invention. Applicants also submit that there are elements of the claimed invention which are not disclosed or suggested by Leppek or Maillard, alone or in combination.

Therefore, Applicants respectfully submit that Leppek and Maillard, either alone or in combination, do not disclose or suggest all of the features of independent claim 1.

On the other hand, Applicants submit that independent claims 24 and 27 also are patentable over the cited references for somewhat similar reasons as those set froth above.

For example, independent claim 24 recites a method of preventing counterfeiting of a smart card, comprising:

> providing a smart card such that none of confidential information and a cryptographic key *for authorizing the smart card*, is carried on the smart card;
> reading said card by a reader such that in each reading, said reader reads only a predetermined small amount of information which makes the card unique (emphasis added).

Independent claim 27 recites a signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for preventing counterfeiting and cloning of smart cards, comprising:

> providing a smart card with a cryptographic structure *for authorizing the smart card* which cannot be accessed completely by a predetermined number of readings,
> wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof (emphasis added).

As mentioned above, the claimed invention, as defined for example by independent claims 1, 24, and 27, does not merely protect the secret of messages, but instead, authenticates or authorizes a smart card in order to prevent counterfeiting and cloning of the smart card. Thus, Applicants respectfully submit that there is a clear and profound difference between the cited references and the claimed invention.

Applicants submit that dependent claims 3-7, 9, 13, and 25 also are patentable over Leppek and Maillard by virtue of their respective dependencies, as well as for the additional features recited therein.

For the foregoing reasons, Applicants respectfully submit that neither Leppek nor Maillard, alone or in combination, discloses or suggests all of the features of claims 1, 3-7, 9, 13, 24, 25, and 27. Therefore, Applicants respectfully request that the Examiner withdraw this rejection.

B. Claims 2, 10-12, 14, 23, and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard, and further in view of Perlman.

In the Response to Arguments, the Examiner stated that:

> *[r]egarding argument (b), examiner disagrees with Applicant. The combination of Leppek/Maillard/Perlman does teach of authenticating/authorizing the smart card. Leppek teaches a plurality of keys so that an intruder cannot arrive at the encryption method easily. Maillard teaches a smart card. Perlman teaches a database that contains valid/invalid cards. These three references combined teach a smart card that is authorized/authenticated by blacklists that may be obtained from a network periodically.*

(see Office Action at page 20, lines 4-10; emphasis added).

Applicants submit, however, that it would not have been obvious to combine Leppek, Maillard, and Perlman to arrive at the claimed invention. Moreover, Applicants submit that, assuming *arguendo* that such references were combined, there are elements of the claimed invention which are not taught or suggested by Leppek, Maillard, or Perlman, either alone or in combination. Therefore, Applicants respectfully traverse this rejection.

For the reasons set forth above, Applicants submit that the Office Action has not established a reasonable motivation for combining Leppek and Maillard to arrive at the claimed invention.

Similarly, Applicants respectfully submit that the Office Action does not establish a reasonable motivation for combining Leppek, Maillard, and Perlman to arrive at the claimed invention.

For example, merely identifying elements from the individual references clearly is *not* sufficient to establish the obviousness of the claimed invention absent some reasonable motivation or suggestion for making the claimed combination.

Thus, merely stating in the Response to Arguments that "*[t]hese three references combined teach a smart card that is authorized/authenticated by blacklists that may be obtained from a network periodically*" (see Office Action at page 20, lines 4-10; emphasis added) without explaining *how* or *why* such a combination would be made, absent the benefit of Applicants' own invention, does not establish a reasonable motivation for making the combination, as a matter of law.

Similarly, merely stating that it would be obvious to combine Perlman with Leppek and Maillard "*because the off-line version of the blacklist provides a listing of all users who are intruders; the periodic updating allows a newer list of intruders to be known, without performing the update constantly - tying up a lot of resources*" (see Office Action at page 9, lines 1-4), without explaining how or why such a combination would be made, absent the benefit of Applicants' own invention, does not establish a reasonable motivation for making the combination, as a matter of law.

Thus, Applicants respectfully submit that Perlman does not make up for the deficiencies of Leppek and Maillard, as set forth above.

Therefore, Applicants submit that claims 2, 10-12, 14, and 23 are patentable over Leppek, Maillard, or Perlman, alone or in combination, at least by virtue of their dependency from independent claim 1.

For somewhat similar reasons, Applicants respectfully submit that Leppek, Maillard, and Perlman, either alone or in combination, do not disclose or suggest the novel and unobvious combination of features recited in independent claim 26.

For example, independent claim 26 recites a system for preventing cloning of a smart card, comprising:

> a smart card such that a cryptographic structure for authorizing the smart card is not carried on the smart card; and
> a reader for reading the smart card and including a database for linking to a network and being updated periodically with a list of unauthorized smart cards,
> wherein said cryptographic structure is kept secret by whoever emits the card or an agent thereof.

As mentioned above, the claimed invention, as defined by independent claim 26, does not merely protect the secret of messages, but instead, authenticates or authorizes the smart cards that are built according to the claimed invention. As such, Applicants respectfully submit that there is a clear and profound difference between the cited references and the claimed invention.

For the foregoing reasons, Applicants respectfully submit that neither Leppek, Maillard, nor Perlman, alone or in combination, discloses or suggests all of the features of claims 2, 10-12, 14, 23, and 26. Therefore, Applicants respectfully request that the Examiner withdraw this rejection.

C. Claims 8, 15-18, and 20-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard, and further in view of Schneier.

Applicants respectfully submit that Schneier does not make up for the deficiencies of Leppek and Maillard, as set forth above.

Therefore, Applicants submit that claims 8, 15-18, and 20-22 are patentable over Leppek, Maillard, or Schneier, alone or in combination, at least by virtue of their dependency from independent claim 1.

For the foregoing reasons, Applicants respectfully submit that Leppek, Maillard, and Schneier, alone or in combination, do not disclose or suggest all of the features of claims 8, 15-18, and 20-22. Therefore, Applicants respectfully request that the Examiner withdraw this rejection.

D. Claim 19 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard, and further in view of Schneier, and further in view of Perlman.

Applicants respectfully submit that Schneier does not make up for the deficiencies of Leppek, Maillard, or Perlman, as set forth above.

Therefore, Applicants submit that claim 19 is patentable over Leppek, Maillard, Perlman, or Schneier, alone or in combination, at least by virtue of its dependency from independent claim 1.

For the foregoing reasons, Applicants respectfully submit that Leppek, Maillard, Schneier, and Perlman, alone or in combination, do not disclose or suggest all of the features of claim 19. Therefore, Applicants respectfully request that the Examiner withdraw this rejection.

III. CONCLUSION

In view of the foregoing, Applicant submits that claims 1-27, all the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: November 30, 2004

John J. Dresch, Esq.
Registration No. 46,672
Sean M. McGinn, Esq.
Registration No. 34,386

McGinn & Gibb, PLLC
8321 Old Courthouse Road, Suite 200
Vienna, VA 22182-3817
(703) 761-4100
Customer No. 21254

CERTIFICATE OF TRANSMISSION

I certify that I transmitted via facsimile to (703) 872-9306 the enclosed Amendment under 37 C.F.R. § 1.116 to Examiner Brandon S. Hoffman on November 30, 2004.

John J. Dresch, Esq.
Registration No. 46,672
Sean M. McGinn, Esq.
Registration No. 34,386